GUIA DE SEGURANÇA

Segurança e Prevenção a Fraude em Estabelecimentos Comerciais

SUMÁRIO

OBJETIVO DA CARTILHA

Evitando surpresas na hora de fechar negócio.

A cartilha de segurança no estabelecimento foi desenvolvido, especialmente, para garantir mais tranquilidade nas negociações realizadas com cartão.

Confira as dicas selecionadas e boas vendas!

1 . SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação deve se estender a toda sua empresa: Na proteção dos dados dos computadores, nos processos do dia-a-dia e na atitude das pessoas.

Investir na segurança dos dados é fundamental para você e seus clientes!

1.1 Proteja o seu computador

Mantenha o equipamento em local protegido e com acesso restrito **(não deixe o computador exposto facilitando o acesso por pessoas não autorizadas)**;

Quando instalar o aplicativo de pagamento TEF, **exija que seu prestador de serviço ative todas as configurações de segurança básicas do seu computador e o oriente como proceder**;

Antivírus - programas utilizados para prevenir, detectar e eliminar vírus de computador;

Firewall - dispositivo que protege um computador ou rede de ataques externos;

Atualizações de segurança do sistema operacional e dos aplicativos instalados;

Acesso remoto - caso seja necessário configurar o acesso remoto, exija a utilização de uma senha forte exclusiva para seu estabelecimento. Se possível ative o acesso remoto somente quando houver manutenção programada e sempre acompanhe estes acessos.

1.2 Dicas práticas de segurança

PEN DRIVE: Não permita o uso da função USB do computador sem o conhecimento de um responsável. Com Pen drives, informações podem ser copiadas ou programas maliciosos podem ser instalados;

Verifique com seu prestador de serviço se é possível a criação de usuário e senha individual para cada funcionário;

Nunca use dados simples como senha (ex: números sequencias ou repetidos , nomes de times, nomes de parentes ou conhecidos, datas importantes, nomes de animais , etc.) pois isso facilita que outras pessoas descubram;

Não divulgue nem compartilhe as senhas;

Adote a política de troca de senha periódica;

Não anote em papel nem imprima relatórios que contenham dados referentes aos cartões dos seus clientes;

Evite o acesso à internet, principalmente se utilizar o computador que possui o aplicativo de pagamento.

1.3 Caso precise acessar a internet

Evite acessar sites que possibilitem a troca de informações, (sites de bate-papo, sites de relacionamento, etc.);

Ao utilizar seu e-mail, não abra mensagens nem clique em anexos ou links de remetentes desconhecidos. Estes podem conter um vírus ou programas que capturam informações;

E-mails de conhecidos, com texto suspeito devem ser verificados pois podem ser falsos. Na dúvida, NÃO clique, apague-os;

Atenção ao phishing (e-mails enviados em nome de grandes instituições para confirmação de compras, dados, cartões): sempre cheque a veracidade da mensagem com a empresa citada antes de clicar em algo;

Cuidado ao fazer downloads, prefira sites conhecidos;

Desconfie de e-mails que prometem prêmios, que enviam fotos, mensagens de amor ou amizade, cartões virtuais, etc. Na dúvida, apague a mensagem;

Não instale programas piratas, pois geralmente vêm com vírus embutidos que podem impactar no desempenho do seu computador e enviar informações pela Internet sem que você saiba.

2. ENGENHARIA SOCIAL

Você já ouviu falar?

2.1 O que é?

Engenharia social é a capacidade de convencer pessoas a fazer coisas que normalmente elas não fariam (por exemplo, fornecer informações a um desconhecido), utilizando técnicas de enganação, persuasão e influência. É uma forma de entrar em organizações, que não necessita da força bruta ou de erros em máquinas.

Para conseguir o que quer, o golpista pode se passar por outra pessoa, assumir outra personalidade, fingir que é um profissional de determinada área, etc.

Cuidado com quem VOCÊ comenta sobre seus dados pessoais ou profissionais!

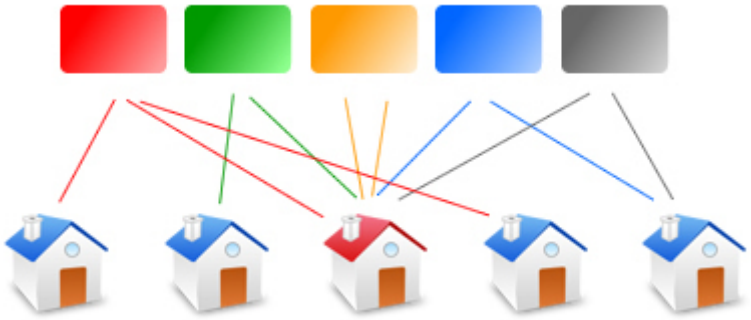
3. COMPROMETIMENTO

Trata-se da captação não autorizada dos dados dos cartões

De posse dessas informações podem ser confeccionados cartões falsos ou os dados podem ser armazenados para posterior utilização fraudulenta, por exemplo via Internet.

3.1 como é identificado um ponto de comprometimento?

Quando o banco reporta transações irregulares feitas com cartões, é realizado um cruzamento de informações para identificar se existe algum ponto em comum entre estes cartões, ou seja, é determinado o local onde os dados foram copiados e a partir daí ocorreram as irregularidades.



como ocorre um comprometimento?

O comprometimento pode ocorrer das seguintes formas:

Aliciamento de funcionários do Estabelecimento:
utilização de um equipamento portátil chamado chupa-cabra ou anotação dos dados do cartão;

Adulteração de equipamento eletrônico:
realizada através de falso técnico;

Utilização de equipamentos ou sistemas TEF em versões não homologadas pelo adquirente principalmente se o TEF que opera via internet não utilizar VPN (Rede Privada Virtual com criptografia) homologada.

4. PREVENÇÃO

O impacto pode ser negativo para a imagem da sua empresa.

4.1 chupa cabra*

Mantenha um cadastro atualizado com os dados de todos os funcionários (dias e horários em que trabalham).

Quando possível anote no verso dos comprovantes de venda o nome do funcionário que efetuou a transação. Caso identifique-se a possibilidade de comprometimento, saberemos quem operou a transação.

Se desconfiar de violação do PinPad (fios, parafusos, selos etc) avise imediatamente a abecs ou o prestador de serviço para retirada e perícia. *Equipamento projetado para leitura, armazenamento e transferência de dados de trilhas magnéticas.

4.2 como evitar a adulteração do equipamento

Faça o inventário periódico dos seus equipamentos;
Realize a fixação dos PIN-Pads e monitore a troca de lugar solicitando justificativas;
Se possível instale um sistema interno de filmagem e armazene esses dados para análise posterior em caso de incidentes confirmados;
Se houver a necessidade de troca do PIN-Pad (seja ele alugado ou próprio) , acione a empresa fornecedora dos equipamentos e não trate com desconhecidos;
Quando possível solicite um relatório sobre a manutenção, assinado pelo técnico;
Se não houver nenhuma solicitação de serviço, não permita a ação e comunique imediatamente os responsáveis

4.3 cuidado com o falso técnico

Na presença de qualquer técnico ou pessoa, mesmo que conhecida, para realizar manutenção, atualização ou troca de hardware, siga algumas recomendações:

Verifique se foi aberto um chamado, quem foi o solicitante e qual o motivo. Na dúvida, entre em contato com seu gestor comercial ou ligue na abecs para confirmação do chamado.
Sempre deixe um responsável acompanhando a ação.

4.4 importante

A informação é o bem mais precioso da sua empresa. Portanto trate-a com responsabilidade para que ela não seja utilizada indevidamente.

Proteger suas informações minimiza a exposição ao risco e as consequências e custos operacionais associados ao comprometimento de dados e fraudes.

Reforçando:
Mantenhas as configurações de segurança do computador e a versão do aplicativo de pagamento TEF sempre atualizados ;
Não deixe pessoas não autorizadas manipularem seu equipamento e em caso de dúvida ou suspeita entre em contato com seu prestador de serviço ou com a abecs, antes de tomar qualquer ação.

Ajude a criar a cultura de Segurança da Informação e divulgar estas dicas !!!!

5. TELEFONES ÚTEIS

Confira os telefones das empresas associadas a abecs, responsáveis pelo credenciamento de estabelecimentos.

Centrais de Relacionamento

Amex

Capitais e regiões metropolitanas: 4004-5040
Demais localidades: 0800 728-5040
Acesse: http://www.americanexpress.com.br/

Cielo

Capitais e regiões metropolitanas: 4002 5472
Demais localidades: 0800 570 8472
Acesse: http://www.cielo.com.br/

GetNet

Capitais e Regiões Metropolitanas: 4002 4000 ou 4003 4000
Demais Localidades: 0800 648 8000
Acesse: http://www.getnet.com.br/

Hipercard

Capitais e Regiões Metropolitanas: 4004-4477
Demais localidades: 0800.728.2222
Acesse: http://www.hipercard.com.br/pj

Redecard

Capitais e regiões metropolitanas: 4001-4422
Demais localidades: 0800-784422
Acesse: http://www.redecard.com.br/

Centrais de Manutenção Técnica

Amex

Capital e regiões metropolitanas: 4004-5010
Demais localidades: 0800 728-510

Cielo

Capitais e regiões metropolitanas: 4002 9111
Demais localidades: 0800 570 0111

GetNet

Capitais e Regiões Metropolitanas: 4002 4000 ou 4003 4000
Demais Localidades: 0800 648 8000

Hipercard

Capitais e Regiões Metropolitanas: 4004-4477
Demais localidades: 0800.728.2222

Redecard

Capitais e regiões metropolitanas: 4001-4433
Demais localidades: 0800-784433